IT-Security (ITS) B1

DIKU, E2022

Today’s agenda

Key Exchange

Key Management

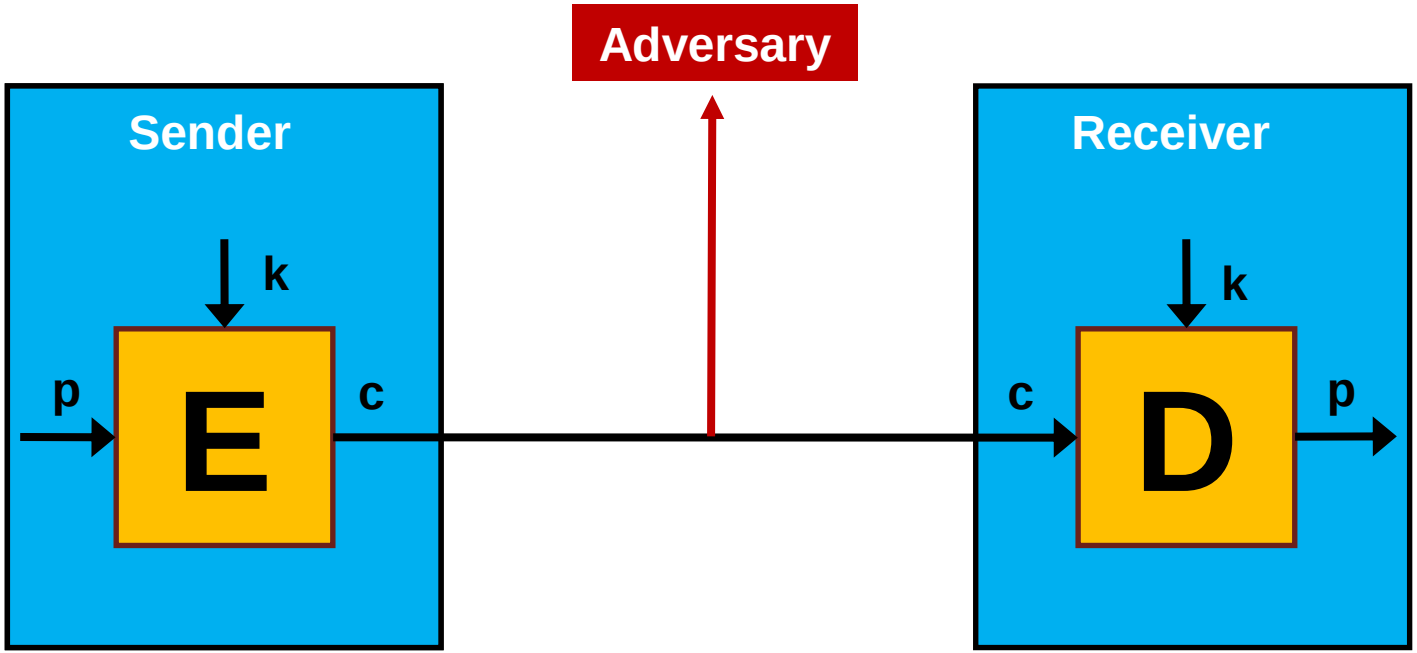
Certificates

Lecture plan

Week	Date	Time	Instructor	Topic	
36	05 Sep	10-12		TL	Security concepts and principles
	09 Sep	10-12		TL	Cryptographic building blocks
37	**12 Sep**	**10-12**		**TL**	**Key establishment and certificate management**
	16 Sep	10-12		CJ	User authentication, IAM
38	19 Sep	10-12		CJ	Operating systems security, web, browser and mail security
	23 Sep	10-12		CJ	IT security management and risk assessment
39	26 Sep	10-12		TL	Software security - exploits and privilege escalation
	30 Sep	10-12		TL	Malicious software
40	03 Oct	10-12		CJ	Firewalls and tunnels, security architecture
	07 Oct	10-12		CJ	Cloud and IoT security
41	10 Oct	10-12		TL	Intrusion detection and network attacks
	14 Oct	10-12		TL	Forensics
42					Fall Vacation - No lectures
43	24 Oct	10-12		CJ	Privacy and GDPR
	28 Oct	10-12		CJ	Privacy engineering
44	31 Oct	10-11		Guest	Special topic
		11-12		TL,CJ	Exam Q/A

https://github.com/diku-its/its-e2022/blob/main/lectureplan2022.md

Recap: Cryptosystems



Recap: Security goals and crypto primitives

Confidentiality, Integrity, Authenticity, Non-repudiation

Stream ciphers, block ciphers, hash functions, asymmetric encryption, hybrid encryption, MACs, digital signatures

Key management

Many keys to protect

Master key

Session key

Signature key

Data encryption key

Key encryption key

...

Protect during entire lifecycle

Generation

Exchange

Storage/backup

Use

Expiration

Revocation

Destruction

Key exchange options include

Pre-distribution

Generated and distributed “ahead of time” e.g. physically

Distribution

Generated by a trusted third party (TTP) and sent to all parties

Agreement

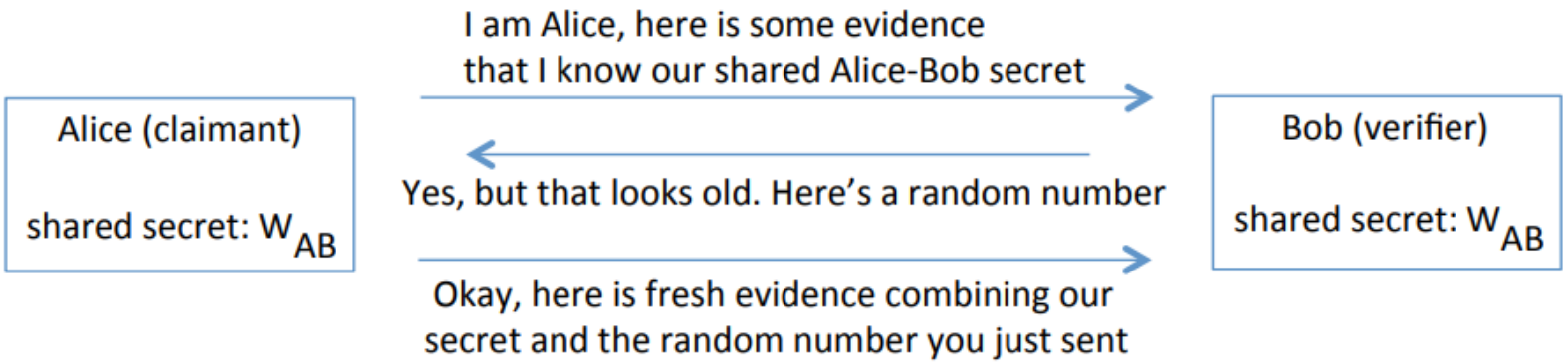
Generated by all parties working together

Asymmetric

Is e really yours?

Key distribution

Basic authenticated key exchange



Developing a key distribution scheme

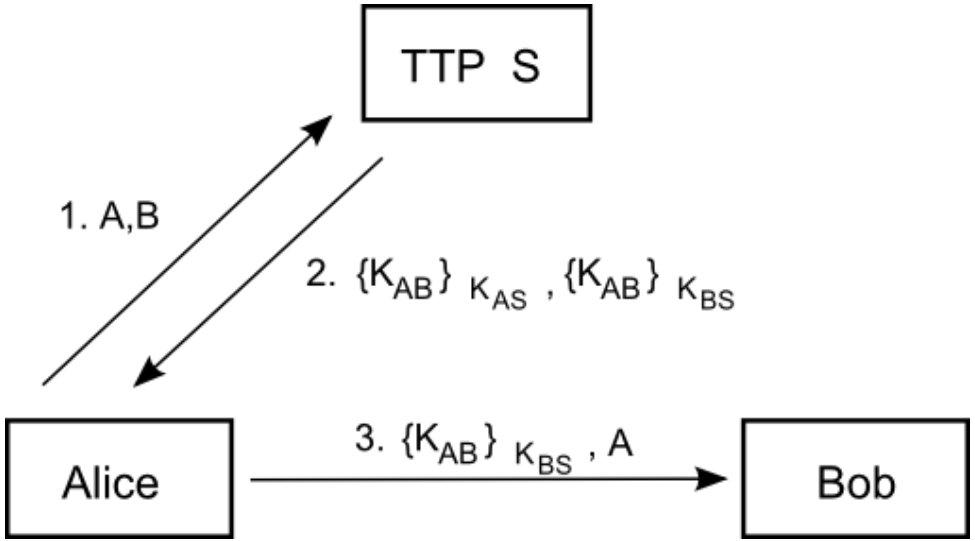
Situation:

- A and B want to exchange keys remotely
- Both A and B share a key (K_AS, K_BS) with a trusted third party, S

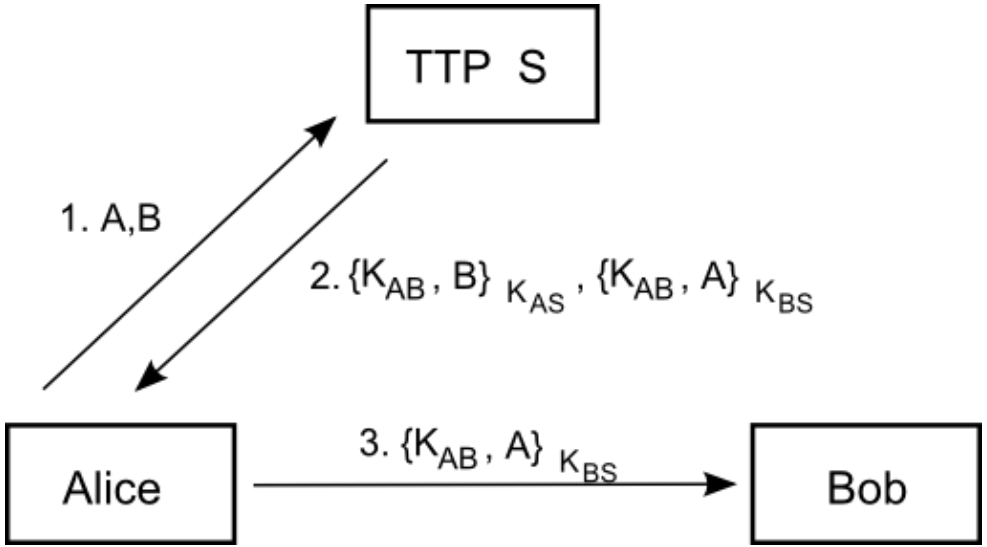
At the end, we want to achieve:

- A and B know a new key K_AB
- No one but A, B, and possibly S knows K_AB
- A and B know that K_AB is newly generated

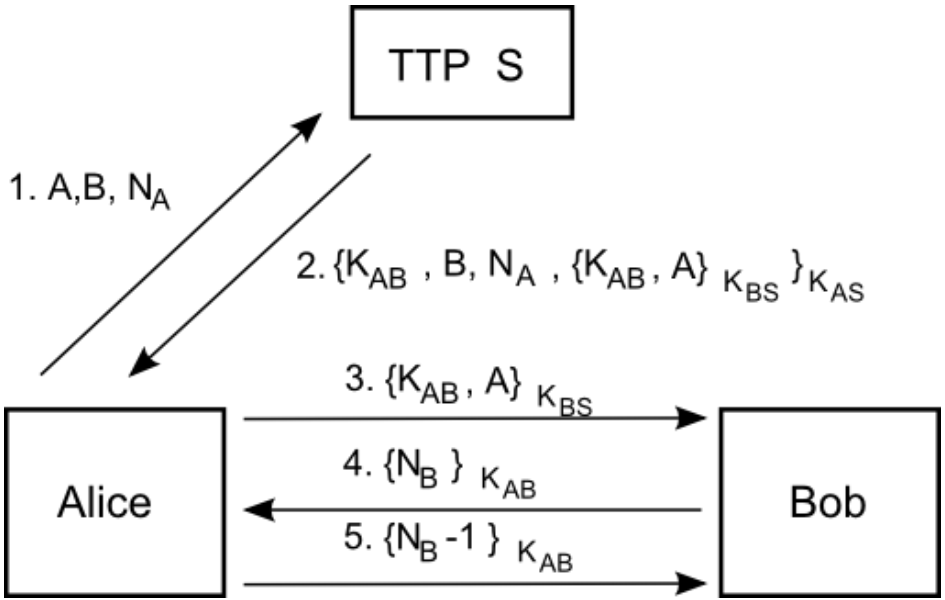
Key distribution



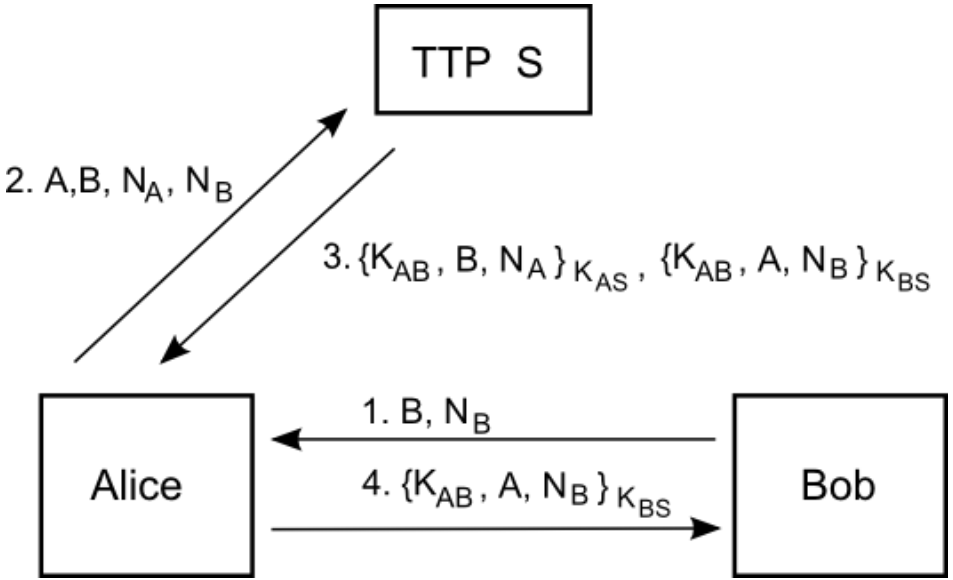
Key distribution



Key distribution



Key distribution



Key agreement

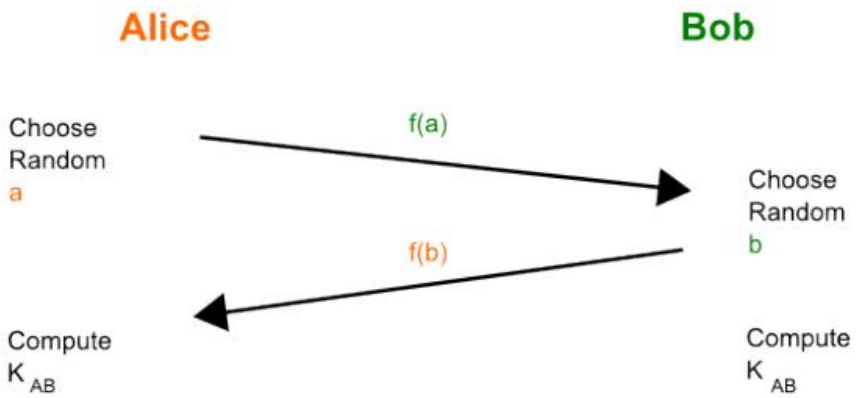
Basic idea

Choose a function f such that

$$f(a,f(b)) = f(b,f(a))$$

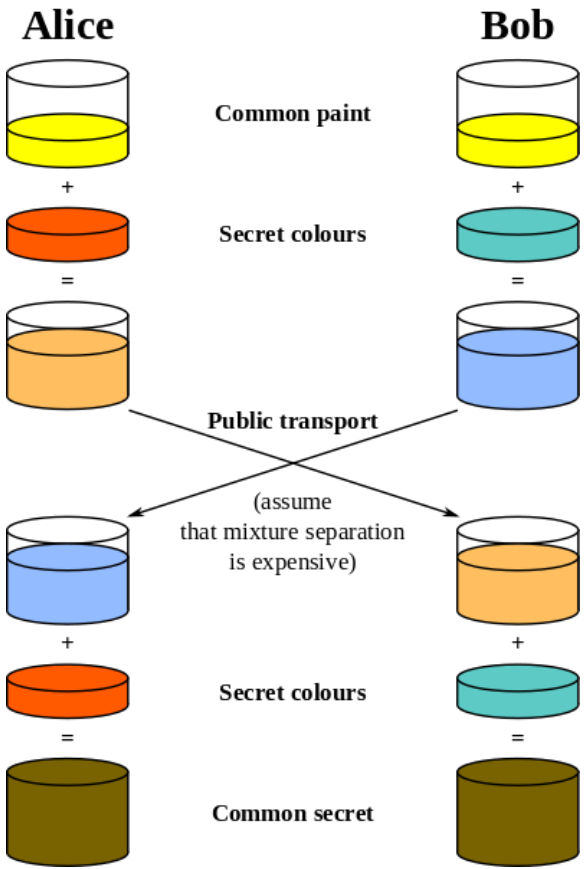
And

$$f^{-1}(x) \text{ is hard}$$



Paint would work

If you wanted to exchange secret paints



Solution by Diffie-Hellman, 1976

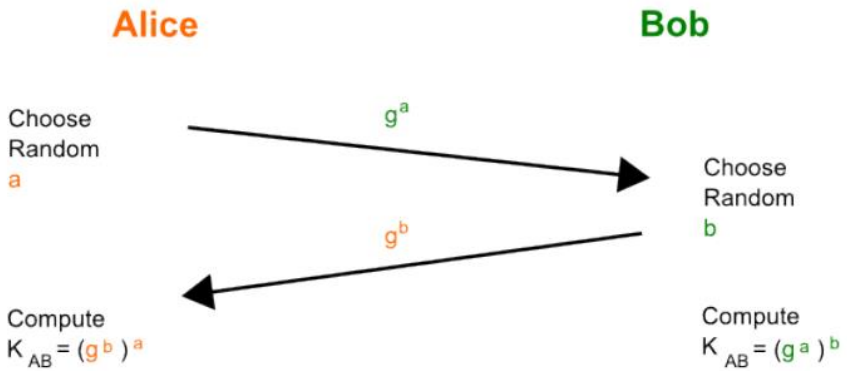
$f(x) = g^x \bmod p$

Given g^a, find x so $g^x = g^a$

Discrete logarithm problem

Given g^a and g^b, find g^{ab}

Computational Diffie-Hellman assumption



Diffie-Hellman: toy example

1. Alice and Bob agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $\mathbf{a = 6}$, then sends Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer $\mathbf{b = 15}$, then sends Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23 = 19$
4. Alice computes $\mathbf{s} = B^a \bmod p$
   - $\mathbf{s} = 19^6 \bmod 23 = \mathbf{2}$
5. Bob computes $\mathbf{s} = A^b \bmod p$
   - $\mathbf{s} = 8^{15} \bmod 23 = \mathbf{2}$
6. Alice and Bob now share a secret (the number **2**).

Diffie-Hellman: toy example (security)

Alice		Bob		Eve	
Known	**Unknown**	**Known**	**Unknown**	**Known**	**Unknown**
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$\mathbf{a = 6}$	$\mathbf{b}$	$\mathbf{b = 15}$	$\mathbf{a}$		$\mathbf{a}, \mathbf{b}$
$A = 5^{a} \bmod 23$		$B = 5^{b} \bmod 23$			
$A = 5^{6} \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$\mathbf{B = 19}$		$\mathbf{A = 8}$		$A = 8, B = 19$	
$\mathbf{s} = B^{a} \bmod 23$		$\mathbf{s} = A^{b} \bmod 23$			
$\mathbf{s} = 19^{6} \bmod 23 = \mathbf{2}$		$\mathbf{s} = 8^{15} \bmod 23 = \mathbf{2}$		$\mathbf{s} = 19^{a} \bmod 23 = 8^{b} \bmod 23$	
$\mathbf{s = 2}$		$\mathbf{s = 2}$			$\mathbf{s}$

Is *e* really yours?

Public-key infrastructure (PKI)

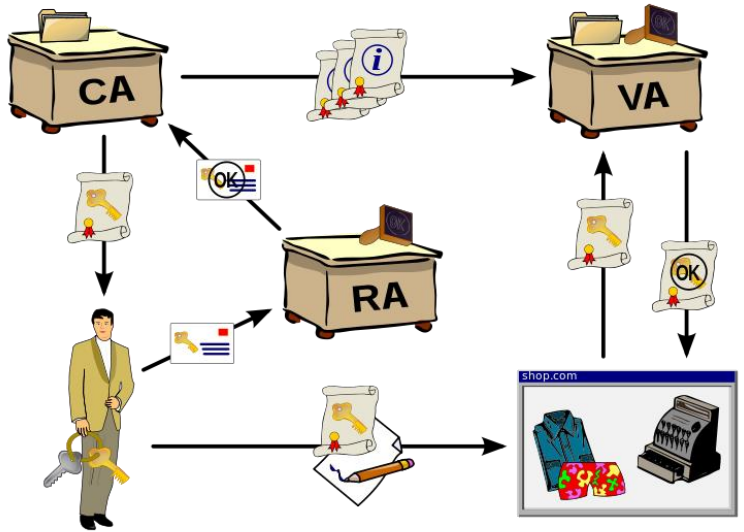
A system for the creation, storage, and distribution of **digital certificates** which are used to verify that a particular public key belongs to a certain entity

X.509 format for certificates include:

Serial number	– unique identification of certificate
Valid-From/To	– lifespan of the certificate
Subject	– the entity/person/machine/etc. identified
Public key	– the entity's public key
Signature	– the actual signature of the issuer

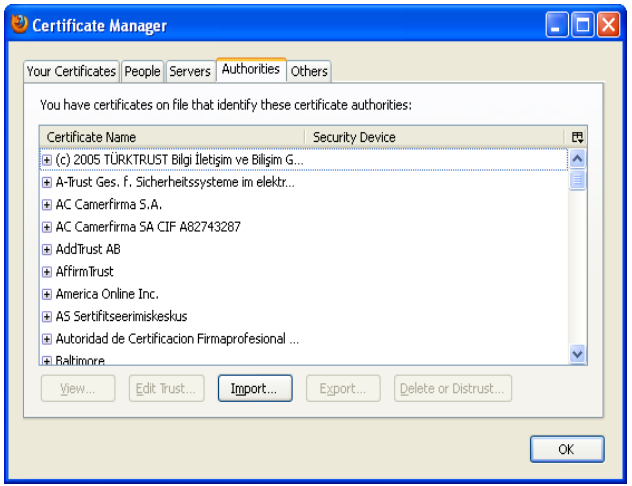
Issuance and verification

A private key is created by you – the certificate owner – when you request your certificate with a Certificate Signing Request (CSR).

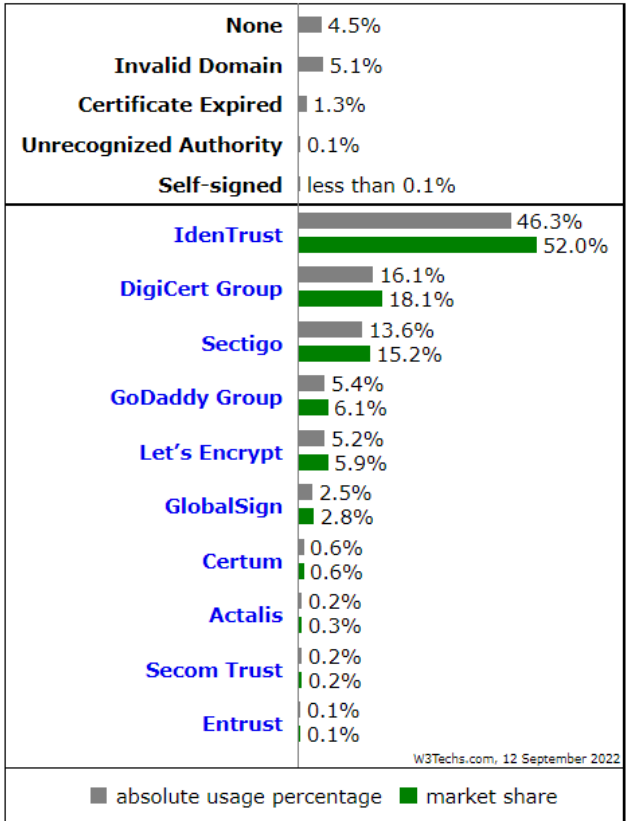


Trust in browsers

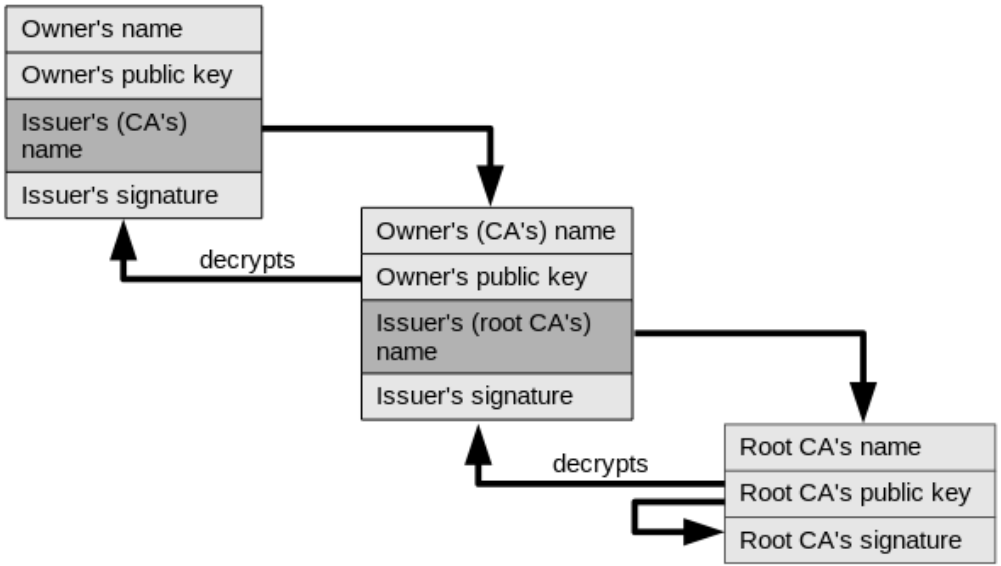
Browsers come pre-configured with a set of root CAs. Do you trust all these CAs (to authenticate properly, to avoid/inform of breaches)?



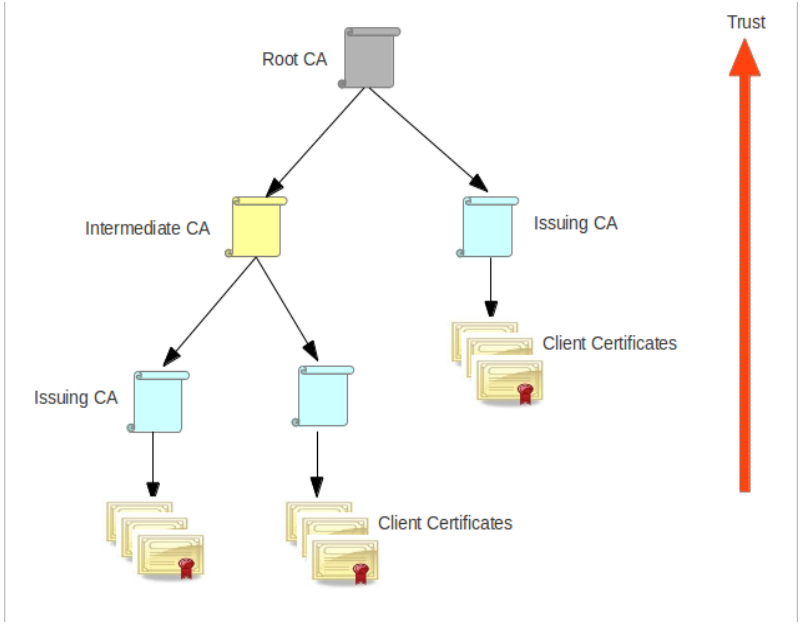
CA providers



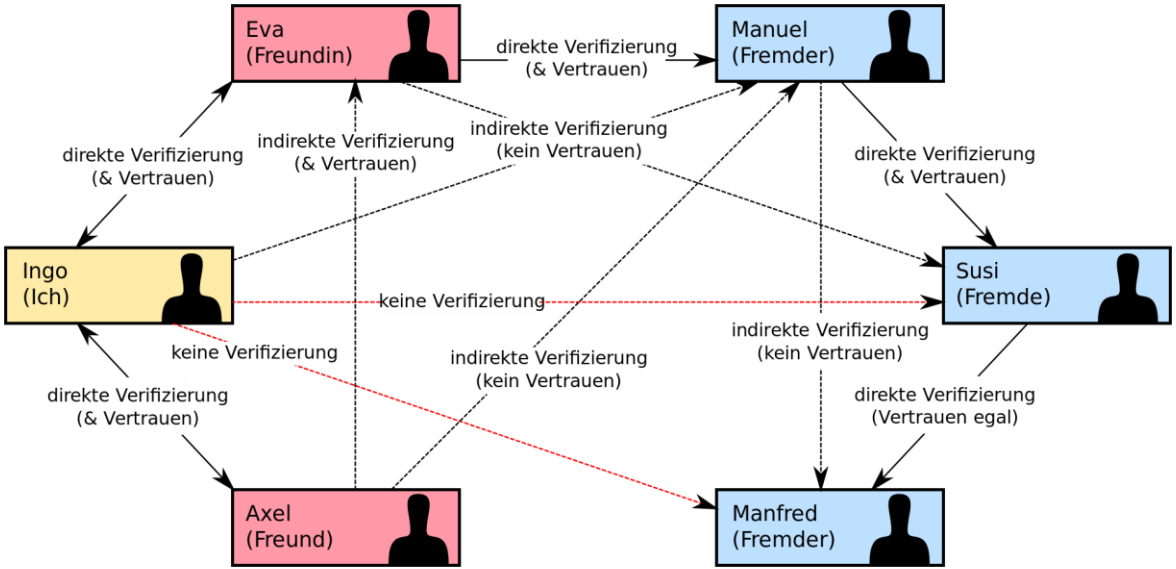
Chain of trust



Types of PKI: CA model



Types of PKI: Web of trust



Revocation of certificates

Certificate revocation list (CRL):

> A list of (serial numbers for) certificates that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted

Online Certificate Status Protocol (OCSP):

> Protocol used for obtaining the revocation status of an X.509 digital certificate

Wrap-up

Lecture plan

Week	Date	Time	Instructor	Topic	
36	05 Sep	10-12		TL	Security concepts and principles
	09 Sep	10-12		TL	Cryptographic building blocks
37	**12 Sep**	**10-12**		**TL**	**Key establishment and certificate management**
	16 Sep	10-12		CJ	User authentication, IAM
38	19 Sep	10-12		CJ	Operating systems security, web, browser and mail security
	23 Sep	10-12		CJ	IT security management and risk assessment
39	26 Sep	10-12		TL	Software security - exploits and privilege escalation
	30 Sep	10-12		TL	Malicious software
40	03 Oct	10-12		CJ	Firewalls and tunnels, security architecture
	07 Oct	10-12		CJ	Cloud and IoT security
41	10 Oct	10-12		TL	Intrusion detection and network attacks
	14 Oct	10-12		TL	Forensics
42					Fall Vacation - No lectures
43	24 Oct	10-12		CJ	Privacy and GDPR
	28 Oct	10-12		CJ	Privacy engineering
44	31 Oct	10-11		Guest	Special topic
		11-12		TL,CJ	Exam Q/A

https://github.com/diku-its/its-e2022/blob/main/lectureplan2022.md